

## **Customer Breach Support**

*A Deloitte managed service*

Notifying, supporting and protecting your customers through a data breach

## Protecting your customers, your brand and your reputation

### The value of a planned breach response

With high profile reports of cyber incidents on the rise and against a backdrop of heightened regulatory scrutiny, few organisations would dispute the value of a pre-planned, customer-centric response to the immediate aftermath of a data breach.

A breach puts your customers at risk of identity theft and fraud. It damages the trust, confidence and loyalty they have in your organisation. It threatens your reputation, your customer base and ultimately your revenue. Even the most well governed organisations can be caught off-guard by increasingly sophisticated cyber attacks.

Deloitte's **Customer Breach Support** service helps clients minimise the impact of a data breach – by putting your customers at the heart of your response and hand holding them through the days and weeks following an incident.

Our comprehensive offering includes customer breach notification plans and communications, and the scalable infrastructure and trained resource to engage, support and protect your customers - and thus your organisation - through the crisis.

### A planned response means....



#### Complying with regulation

The General Data Protection Regulation in Europe mandates that all organisations which process data and offer goods in Europe are in scope.

- Organisations must:
- Report a data breach to the appropriate regulator within 72 hours
  - Have appropriate plans in place to address the breach
  - Notify every affected customer without undue delay



#### Protecting your reputation

Customer trust and loyalty are fragile, and during a crisis depend on how swiftly and effectively an organisation responds to protect the needs of their customers.

Failure to do the right thing - keeping them well informed, supported and provisioned with appropriate identity protection tools and advice, could irreparably damage that trust and loyalty.

The regulator has the power to fine up to **4%** of an organisation's annual global turnover for failure to protect its customers in the event of a data breach.

# Containing the impact of a data breach

## In the event of a breach

An effective data breach response is by its very nature both complex and logistically challenging. When disaster strikes and a breach is uncovered there is little time and rarely the capacity within most organisations to deal with the immediate internal and external impacts whilst simultaneously continuing with 'business as usual' operations.

In our experience, there are five key challenges an organisation faces in the event of a data breach:



### Capacity

Surge capacity must be available at short notice to offer the end customers identity repair and protection, without disrupting an organisations' day to day business



### Speed

Mobilisation of the appropriate outbound customer notification and inbound customer support processes according to the timelines expected by the Regulator and customers



### Communications

Appropriate communication channels, customer messaging, FAQs, call scripting to reach and support customers



### Knowledge

Relevant specialist resource to support customers with identity protection and repair, credit monitoring and fraud alerting



### Coordination

Managing and coordinating the required infrastructure at pace, on top of business as usual

## DATA BREACH IMPACTS 110 MILLION CUSTOMERS WORLDWIDE

### Data compromised:

*110 million customer names, addresses, e-mail addresses, telephone numbers, credit and debit card numbers*

### Impact on company:

*Cost of \$236 million including :*

- *Reputation: 10% drop in share prices*
- *Customer base: 46% drop in year on year sales for that quarter*
- *Loss of Chief Executive Officer*

*An additional \$100 million spent on security post-breach*

...the [data] controller shall communicate the personal data breach to the data subject without undue delay...

# Customer Breach Support by Deloitte

## We offer clients ongoing peace of mind with our comprehensive end to end managed service

From the moment Deloitte is alerted of breach we focus on providing our clients and their customers with a fast and effective service. We notify, support and protect the end consumer and their identities, minimising the potential operational, reputational and financial risks.

Our response is based on a specialist pre-breach programme. We will implement the appropriate strategy, processes, communication materials, resources and capacity, ensuring data is appropriately structured for an outreach. The service guarantees that critical elements of breach response planning are covered in advance of an incident. When a crisis hits, our clients have the right foundations in place to enable us to swiftly take the best possible care of their customers.

### The service

There are two core components to our managed service:

01

## Pre Breach

### Reserved Response Support (RRS)

Under the RRS contract, we provide:

1. A full readiness programme including:
  - Bespoke customer notification and communications strategy
  - Breach notification plan templates and agreed scripts
  - Data analysis for customer outreach
  - Walk through desktop exercise to validate assumptions
  - Simulation exercise to validate plans and test scripts, processes and systems
2. Guaranteed resource and capacity:
  - Customer response forecasting aligned to the customer size and profile
  - Resources including call handling capacity to meet the specific customer scale requirements
  - 24/7 client response
  - Dedicated account manager
  - Full Service Level Agreements

02

## Post Breach

### Live Customer Breach Support

Upon breach activation we provide a dedicated response management team who will coordinate the response to customers, enabling identity protection and remediation services to commence.

This includes:

- A Deloitte "Operations Hub" to coordinate the response
- Implementation of the response strategy, tailored to the specific incident
- Customer outreach infrastructure and resource
- Trained call handling capability
- Specialist identity protection advisory team
- Credit monitoring services
- Fraud alerting / dark web monitoring
- Reporting, analytics and management information

# Deloitte.



Deloitte has 20 years' experience running managed services for our clients, successfully delivering large-scale processing, remediation, data management and customer outreach solutions. Our well-established model combines infrastructure, people, technology and processes into a comprehensive end-to-end managed service delivered by our experienced operations teams.

We have collaborated with AllClear ID, the top US breach response provider\* to leverage their experience and knowledge of successfully responding to over 5000 data breaches. This collaboration creates a unique capability to provide our clients and customers with the response and support required.

\*Forrester 2017

# 1.0 Pre breach: Reserved Response support

## Reserved, guaranteed capacity, pace and specialist support to prepare

Subscribing to the reserved response service ensures organisations have the capability and capacity in place to respond effectively to their customers' needs. A specialist Deloitte team carries out the preparatory phases and our experienced *Operational Hub* delivers the following infrastructure, capacity and breach response procedures:



Once fully on board, we offer clients ongoing peace of mind with our comprehensive end to end managed service. We guarantee the appropriate infrastructure, capacity, skills and logistical reach to respond swiftly and effectively to customer breaches on any scale.

## Components of the breach response service

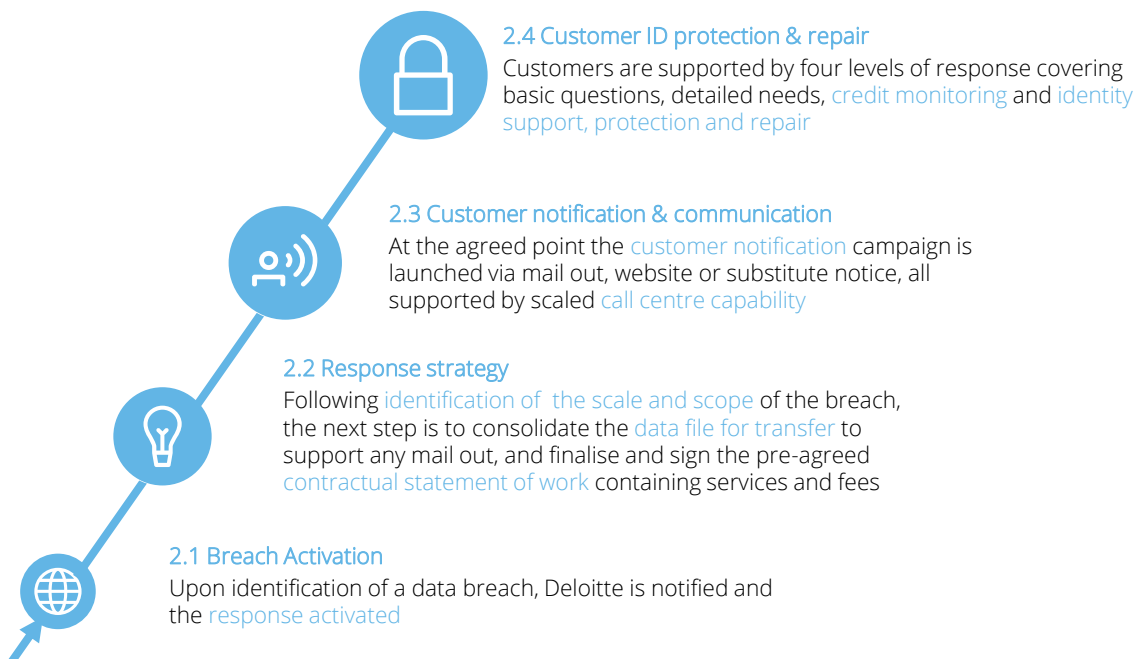
Once accepted onto the reserved response support service, clients unlock retained and scaled access to the full suite of live customer breach response components:

|   |   |   |   |
|---|---|---|---|
|  |  |  |  |
| Dedicated operational hub and account manager                                       | Scalable customer notification capability   | Fraud alert and investigation   | Credit monitoring   |
|  |  |  |  |
| Fully scalable infrastructure   | Reserved call centre at high volume capacity  | Multilingual call centre support  | Identity protection, repair and support   |

## 2.0 Post breach: Live customer support

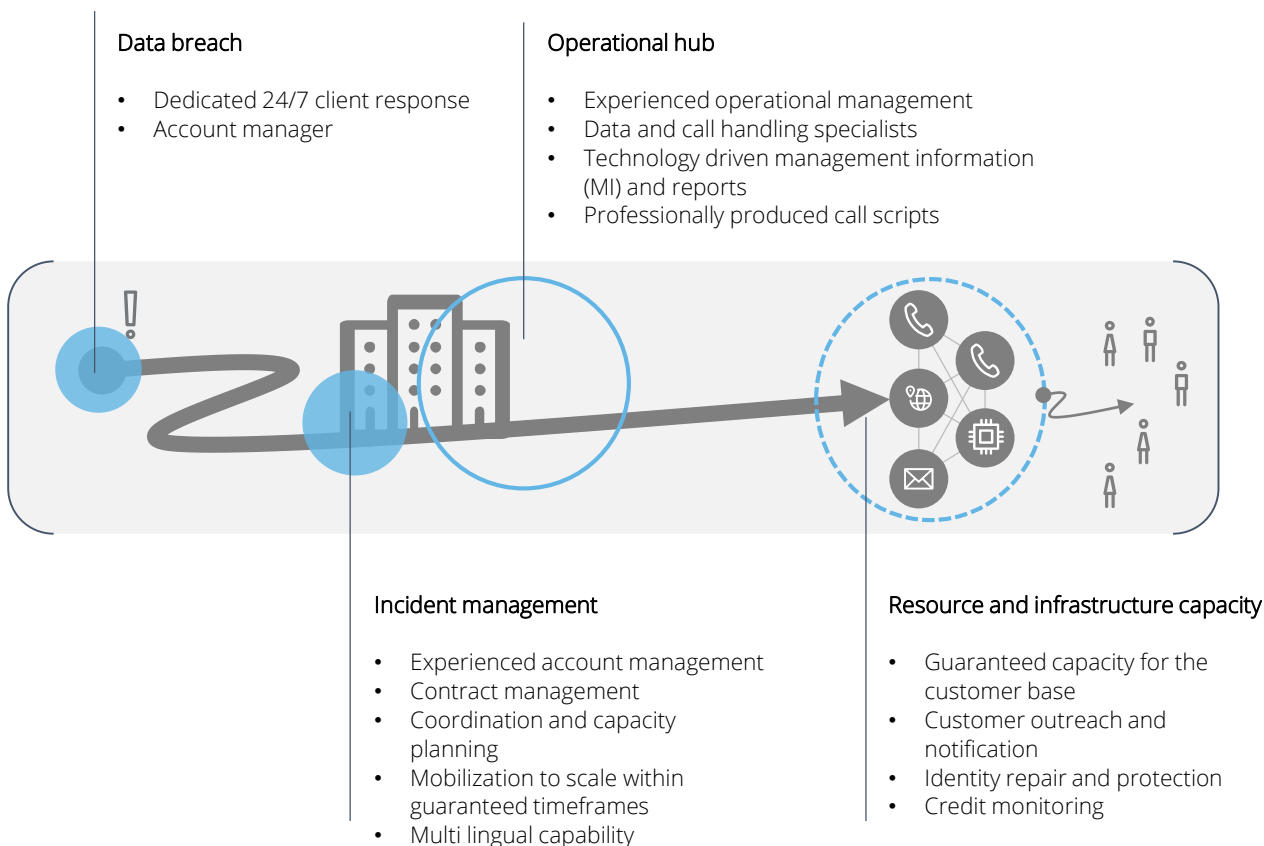
### Pre-planned and controlled support for your customers

In the event of breach response activation, an Incident Management team will mobilise the Operational Hub and coordinate the elements of the service to swiftly support and protect the customer base.



### Components of the breach response service

Our experienced operational hub manages the customer outreach, support, protection and identity repair within agreed timescales to enable customer confidence as well as regulatory compliance.



### The four pillars of our managed service

|   |  |
|---|--|
| <p><b>Cyber specialists</b></p> <p>Experts in cyber security and data protection: Deloitte's dedicated and industry-leading cyber practice operates across the globe. In the UK alone we have <b>delivered security solutions</b> to more than <b>60% of non-restricted FTSE 100 organisations</b>.</p>   | <p><b>Crisis Management</b></p> <p>Deloitte's <b>crisis management</b> services are founded on trust. We build the relationships that make companies all over the world place trust in us to <b>prevent</b> the avoidable and <b>prepare</b> for the truly <b>unavoidable</b>.</p> <p>In the event of a crisis we are able to <b>mobilise</b> our unrivalled network of <b>specialists</b> from risk sensing, agile governance and critical communications to support our clients.</p> |
| <p><b>Established and proven managed services</b></p> <p>Deloitte has <b>20 years' experience</b> of delivering successful, <b>high-quality, large-scale</b> managed services across business sectors including Financial Services, Public Sector, Regulatory Bodies and Corporates. Our operations have supported firms in customer interaction across more than <b>three million customer claims</b>.</p> | <p><b>Collaborating with industry leaders</b></p> <p><i>AllClear ID's</i> award-winning team of <b>experts</b> has been perfecting breach response for <b>more than a decade</b>. <i>AllClear ID</i> has managed <b>thousands of incidents</b>, including three of the four <b>largest data breach responses</b> in history, now safeguarding <b>half a billion customers</b> every day.</p>   |

### Get in touch



**Hugo Morris**  
 Partner, UK  
 Tel: +44 (0) 20 7303 5985  
 hmorris@deloitte.co.uk



**Dominic Cockram**  
 Partner, UK  
 Tel: +44 (0) 20 7303 2288  
 dcockram@deloitte.co.uk

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 264,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication

© 2018. For information, contact Deloitte Touche Tohmatsu Limited.